

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application: 2001年 1月12日

出 願 番 号

Application Number: 特願2001-005147

[ST.10/C]:

[JP2001-005147]

出 願 人

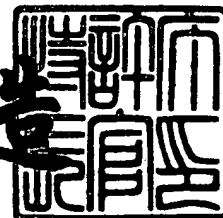
applicant(s): 株式会社エヌ・ティ・ティ・ドコモ

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 3月 1日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2002-3011941

#4

Atty. Docket No. 3815/147



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re Application of :YOSHIMURA, et al.

U.S. Application No. :10/043,546

Group Art Unit: 2131

Filing Date :January 10, 2002

Examiner:

Title ENCRYPTION APPARATUS, DECRYPTION APPARATUS,
 AND AUTHENTICATION INFORMATION ASSIGNMENT
 APPARATUS, AND ENCRYPTION METHOD, DECRYPTION
 METHOD, AND AUTHENTICATION INFORMATION
 ASSIGNMENT METHOD

Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF PRIORITY DOCUMENT

Pursuant to 35 U.S.C. § 119 and 37 CFR § 1.55, Applicants hereby submit a certified copy of the following priority document:

Japanese Patent Application No. 2001-005147, filed January 12, 2001

Applicants hereby enter a claim to the priority of this document.

I certify that this paper, together with any documents referred to as attached or enclosed, are being deposited this date with the United States Postal Service with sufficient postage as first class mail, addressed to the Commissioner of Patents, Washington, D.C., 20231.

Respectfully submitted,

Date: 4-26-02

Ralph F. Hoppin
Ralph F. Hoppin, Reg. No. 38,494
BROWN RAYSMAN MILLSTEIN, FELDER
& STEINER LLP
900 Third Avenue
New York, New York 10022
Tele: (212) 895-2000
Fax : (212) 895-2900

【書類名】 特許願

【整理番号】 DCMH120442

【提出日】 平成13年 1月12日

【あて先】 特許庁長官 殿

【国際特許分類】 H04K 1/00
H04L 9/10

【発明の名称】 暗号化装置および復号装置ならびに認証情報付与装置、
暗号化方法、復号方法、認証情報付与方法

【請求項の数】 17

【発明者】

 【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
 ・ ティ・ティ・ドコモ内

 【氏名】 吉村 健

【発明者】

 【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
 ・ ティ・ティ・ドコモ内

 【氏名】 鈴木 敬

【発明者】

 【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
 ・ ティ・ティ・ドコモ内

 【氏名】 河原 敏朗

【発明者】

 【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ
 ・ ティ・ティ・ドコモ内

 【氏名】 栄藤 稔

【特許出願人】

 【識別番号】 392026693

 【氏名又は名称】 株式会社エヌ・ティ・ティ・ドコモ

【代理人】

【識別番号】 100077481

【弁理士】

【氏名又は名称】 谷 義一

【選任した代理人】

【識別番号】 100088915

【弁理士】

【氏名又は名称】 阿部 和夫

【選任した代理人】

【識別番号】 100106998

【弁理士】

【氏名又は名称】 橋本 傳一

【手数料の表示】

【予納台帳番号】 013424

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9706857

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化装置および復号装置ならびに認証情報付与装置、暗号化方法、復号方法、認証情報付与方法

【特許請求の範囲】

【請求項 1】 送信端末から送信されるメディア情報のビット系列を暗号化して送信する暗号化装置であって、

前記ビット系列の種類を判断する判断手段と、

該判断された前記ビット系列の種類に応じて前記ビット系列の暗号化を行なう暗号化手段と

を備えたことを特徴とする暗号化装置。

【請求項 2】 前記ビット系列の種類は、ビット数または推定の困難性によって区別されることを特徴とする請求項 1 に記載の暗号化装置。

【請求項 3】 前記ビット系列の種類は、暗号が解読された場合の前記メディア情報の復元の困難性によって区別されることを特徴とする請求項 1 に記載の暗号化装置。

【請求項 4】 送信端末から送信されるビット系列を受信する受信手段と、
該受信されたビット系列が暗号化されているか否かを判断する判断手段と、
該判断の結果、前記受信されたビット系列が暗号化されていると判断された場合、前記受信されたビット系列を復号する復号手段と

を備えたことを特徴とする復号装置。

【請求項 5】 前記復号手段により復号されたビット系列を受信端末へ送信する送信手段を更に備えたことを特徴とする請求項 4 に記載の復号装置。

【請求項 6】 送信端末から送信されるメディア情報のビット系列に認証情報を付与して送信する認証情報付与装置であって、

前記ビット系列の種類を判断する判断手段と、

該判断された前記ビット系列の種類に応じて前記認証情報の付与を行なう認証付与手段と

を備えたことを特徴とする認証情報付与装置。

【請求項 7】 前記ビット系列の種類はビット数または改竄時の影響度合い

によって区別されることを特徴とする請求項 6 に記載の認証情報付与装置。

【請求項 8】 送信端末から送信されるビット系列を受信する受信手段と、
該受信されたビット系列に認証情報が付与されているか否かを判断する判断手段と、

該判断の結果、前記受信されたビット系列に認証情報が付与されていると判断された場合、前記受信されたビット系列に基づく認証を行なう認証手段と
を備えたことを特徴とする認証装置。

【請求項 9】 前記認証手段による認証の結果を通知する通知手段を更に備えたことを特徴とする請求項 8 に記載の認証装置。

【請求項 10】 前記認証手段による認証の結果、正当であると判断されたビット系列を受信端末へ送信する送信手段を更に備えたことを特徴とする請求項 8 または 9 に記載の認証装置。

【請求項 11】 送信端末から送信されるメディア情報のビット系列を暗号化して送信する暗号化装置により実行される暗号化方法であって、

前記ビット系列の種類を判断する判断ステップと、
該判断された前記ビット系列の種類に応じて前記ビット系列の暗号化を行なう暗号化ステップと

を備えたことを特徴とする暗号化方法。

【請求項 12】 送信端末から送信されるビット系列を復号装置により受信する受信ステップと、

該受信されたビット系列が暗号化されているか否かを判断する判断ステップと

、
該判断の結果、前記受信されたビット系列が暗号化されていると判断された場合、前記受信されたビット系列を復号する復号ステップと

を備えたことを特徴とする復号方法。

【請求項 13】 前記復号ステップにおいて復号されたビット系列を前記復号装置から受信端末へ送信する送信ステップを更に備えたことを特徴とする請求項 12 に記載の復号方法。

【請求項 14】 送信端末から送信されるメディア情報のビット系列に認証

情報を付与して送信する認証情報付与装置により実行される認証情報付与方法であって、

前記ビット系列の種類を判断する判断ステップと、

該判断された前記ビット系列の種類に応じて前記認証情報の付与を行なう認証付与ステップと

を備えたことを特徴とする認証情報付与方法。

【請求項 1 5】 送信端末から送信されるビット系列を復号装置により受信する受信ステップと、

該受信されたビット系列に認証情報が付与されているか否かを判断する判断ステップと、

該判断の結果、前記受信されたビット系列に認証情報が付与されていると判断された場合、前記受信されたビット系列に基づく認証を行なう認証ステップとを備えたことを特徴とする認証方法。

【請求項 1 6】 前記認証ステップにおける認証の結果を通知する通知ステップを更に備えたことを特徴とする請求項 1 5 に記載の認証方法。

【請求項 1 7】 前記認証ステップにおける認証により正当であると判断されたビット系列を復号装置から受信端末へ送信する送信ステップを更に備えたことを特徴とする請求項 1 5 または 1 6 に記載の認証方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、選択的に暗号化処理または認証処理を行なう暗号化装置および認証情報付与装置ならびに暗号化方法、復号方法、認証情報付与方法に関する。

【0 0 0 2】

【従来の技術】

通信システムにおいて伝送される音声情報や画像情報等のメディア情報のビット系列をブロック暗号を用いて暗号化する方式では、従来、たとえば図 1 に示すように、元のビット系列（パケット）をブロック長の整数倍に合わせるために、0 ビットを付加する（パディング）。そして、パディングが行なわれたビット系

列について、暗号鍵を使用してビット列の変換を行なっている。

【0003】

このようにして暗号化して送信されたビット系列は、受信側で復号鍵を使用して変換され、元のビット系列に復号される。

【0004】

また、暗号化方式を応用して認証処理を行なう場合は、図2に示すように、元のビット系列を一方向性関数で変換した値を認証鍵により暗号化した認証情報を、元のビット系列に付加して送信する。

【0005】

一方、受信側では、受信した元のビット系列に対して同一の一方向性関数を用いて求めた値を作成する。そして、作成された値と受信したビット系列を検査鍵で復号した結果との一致を判断して、受信したビット系列の送信元の正当性を確認する。

【0006】

メディア情報のビット系列についてこのような暗号処理や認証処理を行なう手法として、たとえば特開平2000-59323号公報には、重要でないデータの認証に多くの時間を要する問題を改善する技術が開示されている。この技術では、送信ユニットによりデジタルAVデータの重要度を判断し、その判断結果に応じて認証ルールを選択が行なわれる。

【0007】

また、特開平5-56034号公報には、デジタル信号の伝送路で所定の秘匿コードに従ってデジタル信号の秘匿化を行なう技術が開示されている。この技術によれば、アナログ音声信号の無音状態を検出し、その検出結果に基づいてデジタル信号の秘匿コードを逐次変更することにより、秘匿の解読を防止する。

【0008】

【発明が解決しようとする課題】

しかしながら、上述した従来の暗号化方式または認証方式では、ビット数の少ないビット系列や容易に推定出来るビット系列に対してまで暗号化または認証処理を行なっている。このため、元のビット系列を総当りで計算すれば、容易に暗

号文から平文を解読される。つまり、解読を試みる攻撃者が容易に平文と暗号文の対を入手可能であり、鍵が破られやすくなるという問題があった。

【0009】

また、送信する全てのビット系列について暗号化処理や認証処理を行なうと、オーバーヘッドが増加すると共に、処理遅延が増加するという問題があった。

【0010】

また、上述した従来の暗号化方式または認証方式では、暗号化によるパディングや、認証情報の付加により、送信する情報量が増大するという問題があった。

【0011】

さらに、メディア情報の暗号化や認証に関する従来の手法では、送信するコンテンツ毎の重要度の判断処理や、秘匿コードを逐次変更する処理のために、オーバーヘッドが増大するという問題があった。

【0012】

本発明は、上記問題に鑑みてなされたものであり、その目的とするところは、暗号鍵や認証鍵が破られるのを防ぐことができる暗号化装置および認証情報付与装置ならびに暗号化方法、認証情報付与方法を提供することにある。

【0013】

また、本発明の目的は、暗号処理や認証処理のためのオーバーヘッドを軽減することができる暗号化装置および認証情報付与装置ならびに暗号化方法、認証情報付与方法を提供することにある。

【0014】

さらに、本発明の目的は、暗号化や認証情報付加による情報量の増大を抑制することができる暗号化装置および復号装置ならびに認証情報付与装置、暗号化方法、復号方法、認証情報付与方法を提供することにある。

【0015】

【課題を解決するための手段】

このような目的を達成するために、請求項1に記載の発明は、送信端末から送信されるメディア情報のビット系列を暗号化して送信する暗号化装置であって、前記ビット系列の種類を判断する判断手段と、該判断された前記ビット系列の種

類に応じて前記ビット系列の暗号化を行なう暗号化手段とを備えたことを特徴とする。

【0016】

これにより、暗号鍵が破られることを防止できるとともに、暗号処理の計算量を低減することができる。また、暗号処理に伴う情報量の増大を防止することができる。

【0017】

また、請求項2に記載の発明は、請求項1に記載の暗号化装置において、前記ビット系列の種類は、ビット数または推定の困難性によって区別されることを特徴とする。

【0018】

したがって、第三者から覗かれても良いビット系列については暗号化を行なうことなくそのまま伝送することにより、暗号鍵が破られることを回避できる。

【0019】

また、請求項3に記載の発明は、請求項1に記載の暗号化装置において、前記ビット系列の種類は、暗号が解読された場合の前記メディア情報の復元の困難性によって区別されることを特徴とする。

【0020】

従って、暗号化処理に伴うオーバーヘッドやパディングによる情報量の増大を抑制することができる。

【0021】

また、請求項4に記載の発明は、復号装置であって、送信端末から送信されるビット系列を受信する受信手段と、該受信されたビット系列が暗号化されているか否かを判断する判断手段と、該判断の結果、前記受信されたビット系列が暗号化されていると判断された場合、前記受信されたビット系列を復号する復号手段とを備えたことを特徴とする。

【0022】

これにより、選択的に暗号化されたビット系列を、そのビット系列の種類に基づいて復号することが出来る。

【0023】

また、請求項5に記載の発明は、請求項4に記載の復号装置において、前記復号手段により復号されたビット系列を受信端末へ送信する送信手段を更に備えたことを特徴とする。

【0024】

したがって、復号装置自身が受信端末である場合のみならず、受信装置とは別体の復号装置としても本発明を実施することができる。

【0025】

また、請求項6に記載の発明は、認証情報付与装置であって、送信端末から送信されるメディア情報のビット系列に認証情報を付与して送信する認証情報付与装置であって、前記ビット系列の種類を判断する判断手段と、該判断された前記ビット系列の種類に応じて前記認証情報の付与を行なう認証付与手段とを備えたことを特徴とする。

【0026】

これにより、認証鍵が破られることを防止できるとともに、認証情報付与についての計算量を低減することができる。また、認証情報付与に伴う情報量の増大を抑えることができる。

【0027】

また、請求項7に記載の発明は、請求項6に記載の認証情報付与装置において、前記ビット系列の種類はビット数または改竄時の影響度合いによって区別されることを特徴とする。

【0028】

したがって、第三者から改竄されても良いビット系列については認証情報を付与することなくそのまま伝送することにより、認証鍵が破られることを回避できる。

【0029】

また、請求項8に記載の発明は、認証装置であって、送信端末から送信されるビット系列を受信する受信手段と、該受信されたビット系列に認証情報が付与されているか否かを判断する判断手段と、該判断の結果、前記受信されたビット系

列に認証情報が付与されていると判断された場合、前記受信されたビット系列に基づく認証を行なう認証手段とを備えたことを特徴とする。

【 0 0 3 0 】

これにより、選択的に認証情報が付与されたビット系列を、そのビット系列の種類に応じて認証を行なうことが出来る。

【 0 0 3 1 】

また、請求項 9 に記載の発明は、請求項 8 に記載の認証装置において、前記認証手段による認証の結果を通知する通知手段を更に備えたことを特徴とする。

【 0 0 3 2 】

したがって、認証確認以降パケットそのものを処理せず、単に認証結果が正当であるかどうかのみを通知することが可能となる。

【 0 0 3 3 】

また、請求項 1 0 に記載の発明は、請求項 8 または 9 に記載の認証装置において、前記認証手段による認証の結果、正当であると判断されたビット系列を受信端末へ送信する送信手段を更に備えたことを特徴とする。

【 0 0 3 4 】

したがって、認証装置自身が受信端末である場合のみならず、受信装置とは別体の認証装置としても本発明を実施することができる。

【 0 0 3 5 】

また、請求項 1 1 に記載の発明は、送信端末から送信されるメディア情報のビット系列を暗号化して送信する暗号化装置により実行される暗号化方法であって、前記ビット系列の種類を判断する判断ステップと、該判断された前記ビット系列の種類に応じて前記ビット系列の暗号化を行なう暗号化ステップとを備えたことを特徴とする。

【 0 0 3 6 】

また、請求項 1 2 に記載の発明は、復号方法であって、送信端末から送信されるビット系列を復号装置により受信する受信ステップと、該受信されたビット系列が暗号化されているか否かを判断する判断ステップと、該判断の結果、前記受信されたビット系列が暗号化されていると判断された場合、前記受信されたビッ

ト系列を復号する復号ステップとを備えたことを特徴とする。

【0037】

また、請求項13に記載の発明は、請求項12に記載の復号方法において、前記復号ステップにおいて復号されたビット系列を前記復号装置から受信端末へ送信する送信ステップを更に備えたことを特徴とする。

【0038】

また、請求項14に記載の発明は、送信端末から送信されるメディア情報のビット系列に認証情報を付与して送信する認証情報付与装置により実行される認証情報付与方法であって、前記ビット系列の種類を判断する判断ステップと、該判断された前記ビット系列の種類に応じて前記認証情報の付与を行なう認証付与ステップとを備えたことを特徴とする。

【0039】

また、請求項15に記載の発明は、認証方法であって、送信端末から送信されるビット系列を復号装置により受信する受信ステップと、該受信されたビット系列に認証情報が付与されているか否かを判断する判断ステップと、該判断の結果、前記受信されたビット系列に認証情報が付与されていると判断された場合、前記受信されたビット系列に基づく認証を行なう認証ステップとを備えたことを特徴とする。

【0040】

また、請求項16に記載の発明は、請求項15に記載の認証方法において、前記認証ステップにおける認証の結果を通知する通知ステップを更に備えたことを特徴とする。

【0041】

さらに、請求項17に記載の発明は、請求項15または16に記載の認証方法において、前記認証ステップにおける認証により正当であると判断されたビット系列を復号装置から受信端末へ送信する送信ステップを更に備えたことを特徴とする。

【0042】

【発明の実施の形態】

以下、図面を参照し、本発明の実施形態について詳細に説明する。

【0043】

(第1実施形態)

図3は、本発明を適用した通信システムに使用される暗号化／認証付与装置の構成の一例を示す図であり、本発明に関係する部分のみを概念的に示している。

【0044】

本実施形態に係る暗号化／認証付与装置100は、送信端末に組み込まれていても良く、送信端末とは別体として構成されても良い。また、暗号化／認証付与装置100は、送信端末と受信端末との間に位置する無線基地局等の各ノードとして構成されても良い。

【0045】

暗号化／認証付与装置100は、送信端末から送信するメディア情報のビット系列に対する暗号化、または認証情報の付与を選択する暗号・認証選択部102と、ビット系列の暗号化を行なう暗号化部104と、ビット系列に認証情報を付与する認証付与部106とから構成される。

【0046】

暗号・認証選択部102では、送信端末から送信するビット系列の種類が判断され、暗号化を行なうものと判断された場合、当該ビット系列が暗号化部104へ渡される。また、認証情報を付与すべきものと判断された場合、当該ビット系列は認証付与部106へ渡される。判断の結果、暗号または認証を行なわないビット系列であると判断された場合は、当該ビット系列について変換処理が行なわれることなくそのまま送信される。

【0047】

なお、暗号化／認証付与装置100は、請求項に記載の暗号化装置または認証情報付与装置として機能する。

【0048】

次に、このように構成された暗号化／認証付与装置100の動作の一例について、図4を参照して詳細に説明する。

【0049】

本実施形態では、暗号化や認証情報の種類は、ビット数または推定の困難性によって区別され、送信するパケットの中でもビット数の少ないビット系列や容易に推定出来る特定のビット系列に対しては、暗号化や認証情報の付与は行なわない。

【0050】

図4に示す例では、送信端末300から受信端末400へ音声ストリームが送信されており、この音声ストリームのビット系列には、有音部302と、無音部304とが含まれている。ここで、無音部304には、雑音情報等が入っており、パケット長が短い。従って、この部分の暗号文を攻撃されると、容易に暗号が破られることとなる。

【0051】

そこで、有音部302には暗号化または認証情報の付与を行なう一方、無音部304には暗号化や認証情報の付加を行わず、そのまま伝送する。この選択処理は、図3に示す暗号化／認証付与装置100の暗号・認証選択部102において、送信するパケット毎に有音部であるか無音部であるかを判断することにより行なう。

【0052】

このように、ビット系列の種類に応じて選択的に暗号化または認証情報の付与を行なうことにより、暗号鍵や認証鍵を破られることを避けるとともに、オーバーヘッドの増加を抑制できる。

【0053】

(第2実施形態)

本実施形態では、メディア情報のビット系列の種類は、暗号が解読された場合のメディア情報の復元の困難性によって区別され、複数のパケットのうちの一部だけが解読されても元のメディア情報の復元には難しいビット系列は暗号化を行なわない。本実施形態もまた、上述の実施形態と同様に図3に示す暗号化／認証付与装置100を使用することができる。

【0054】

以下、図5を参照し、図3に示すように構成された暗号化／認証付与装置10

0の動作の一例について詳細に説明する。

【0055】

図5(a)に示す例では、送信端末300から受信端末400へMPEG1により動画情報を送信する。MPEG1では、動画像の双方向予測（未来再生画像からの逆方向予測及び過去再生画像からの順方向予測）を行なうために、Iピクチャ406、Pピクチャ402、およびBピクチャ404という3つの画像タイプが規定されている。この3つの画像タイプのうち、Iピクチャ406はフレーム内符号化画像であり、この画像タイプのビット系列が攻撃を受けた場合は、容易に元のビット系列が復元される可能性がある。一方、Pピクチャ402及びBピクチャ404は予測符号化画像であり、複数の動画像間の差分のデータである。したがって、このビット系列のみを解読されても、元のメディア情報を復元することは困難である。

【0056】

そこで、図3に示す暗号化／認証付与装置100の暗号・認証選択部102において、送信する動画像データの画像タイプを判断する。そして、Iピクチャ406の場合は暗号化部104で暗号化を行なう一方、Pピクチャ402およびBピクチャ404については暗号化を行わず、そのまま伝送する。

【0057】

このような処理を行なうことにより、暗号化処理のオーバーヘッドやパディングによる情報量の増大を抑制することができる。

【0058】

なお、本実施形態ではMPEG1を例に挙げて説明したが、MPEG1と同様にIピクチャ、Pピクチャ、Bピクチャなどの異なるピクチャタイプを使用するMPEG2やMPEG4についても、本発明を適用することが可能である。

【0059】

本実施形態の応用例としては、以下のものを挙げることができる。

【0060】

ファイルを複数パケットで転送する場合、図5(b)に示すように、1パケットのみを暗号化して転送する。この場合、暗号化されていないパケットに含まれ

る情報だけでは元のファイルを復元することができない。暗号化する部分としては、例えばファイル圧縮のためのコンフィギュレーション情報を含むパッケージが挙げられる。その場合、残りのパッケージからでは当該ファイルを元どおりに伸張することが不可能である。

【0061】

また、ビット系列の種類をビット数または改竄時の影響度合いによって区別し、一部だけ改竄されても大きな影響を与えないビット系列に対しては、認証情報を付与しないように選択処理を行なう。たとえば、ユーザ情報、課金情報、コンフィギュレーション情報、映像ストリームのIピクチャ、階層符号化ストリームのベースレイヤなどには認証情報を付与する。一方、音声ストリームの無音情報、PピクチャやBピクチャ、階層符号化における上位送の画像などは、認証情報を付与しない。

【0062】

例えば、映像や音声、音響の符号化を階層化する場合、ベースレイヤだけでもある程度のメディア品質を提供することができるが、エンハンスレイヤだけでは意味がなく、ベースレイヤとエンハンスレイヤを組み合わせることによって更に高いメディア品質を提供することができる。そこで、ベースレイヤのみを暗号化する一方、エンハンスレイヤについては暗号化を行わずにそのまま伝送する。

【0063】

階層符号化には、異なる空間解像度（ベースレイヤはQCIF、エンハンスレイヤはCIF、など）で階層化する場合や、異なる時間解像度（ベースレイヤは10frame/s、エンハンスレイヤは20frame/s、など）で階層化する場合が考えられる。

【0064】

このような処理を行なうことにより、暗号化処理のオーバーヘッドやパディングによる情報量の増大を抑制することができる。

【0065】

（第3実施形態）

図6は、本発明を適用した通信システムに使用される復号／認証装置の構成の

一例を示す図であり、本発明に係る部分のみを概念的に示している。

【0066】

復号／認証装置200は、受信端末に組み込まれていても良い。また、受信端末とは別体として構成されても良い。さらに、送信端末と受信端末との間に位置する無線基地局等の各ノードとして構成されても良い。

【0067】

復号／認証装置200は、受信したビット系列に認証情報が付与されていることを検出するための認証検出部202と、受信したビット系列についての認証を行なうための認証確認部204と、受信したビット系列が暗号化されていることを検出するための暗号検出部206と、受信したビット系列が暗号化されている場合に復号処理を行なうための暗号復号部208とから構成される。

【0068】

復号／認証装置200によって受信されたビット系列は、認証検出部202において認証情報の検出が行なわれ、検出された場合は認証確認部204へ当該ビット系列が渡される。認証情報の検出が行なわれなかったビット系列、および認証確認部204において認証が認められたビット系列は、暗号検出部206へ渡される。暗号検出部206では、ビット系列が暗号化されているか否かの検出処理が行なわれる。暗号情報が含まれている場合は、受信したビット系列が暗号復号部208へ渡されて復号が行なわれた後、受信端末へ送信される。暗号検出部206において、ビット系列が暗号化されていることが認識されなかった場合は、受信したビット系列がそのまま受信端末へ渡される。

【0069】

認証検出部202における認証情報の検出、および暗号検出部206における暗号化の有無の検出は、たとえばIPによって情報を転送する場合は、受信したデータに付加されているIPヘッダを参照することにより行なう。すなわち、IPヘッダ内の「プロトコル」に含まれるプロトコル番号を参照して、そのビット系列が暗号化されているか、あるいは認証情報が付与されているかを知ることができる。また、RTP(Real-time Transport Protocol)ヘッダ内の「ペイロードタイプ」により識別することも可能である。

【 0 0 7 0 】

(第 4 実施形態)

本実施形態では、図 3 の暗号化／認証付与装置 1 0 0 と、図 6 の復号／認証装置 2 0 0 とを組み合わせ使用する場合について説明する。

【 0 0 7 1 】

送信端末 1 0 0 の暗号・認証選択部 1 0 2 では、送信端末から送信するビット系列の種類が判断され、暗号化を行なうものと判断された場合、当該ビット系列が暗号化部 1 0 4 へ渡される。また、認証情報を付与すべきものと判断された場合、当該ビット系列は認証付与部 1 0 6 へ渡される。判断の結果、暗号または認証を行なわないビット系列であると判断された場合は、当該ビット系列について変換処理が行なわれることなくそのまま送信される。

【 0 0 7 2 】

一方、復号／認証装置 2 0 0 によって受信されたビット系列は、認証検出部 2 0 2 において認証情報の検出が行なわれ、検出された場合は認証確認部 2 0 4 へ当該ビット系列が渡される。認証情報の検出が行なわれなかったビット系列、および認証確認部 2 0 4 において認証が認められたビット系列は、暗号検出部 2 0 6 へ渡される。暗号検出部 2 0 6 では、ビット系列が暗号化されているか否かの検出処理が行なわれる。暗号情報が含まれている場合は、受信したビット系列が暗号復号部 2 0 8 へ渡されて復号が行なわれた後、受信端末へ送信される。暗号検出部 2 0 6 において、ビット系列が暗号化されていることが認識されなかった場合は、受信したビット系列がそのまま受信端末へ渡される。

【 0 0 7 3 】

(他の実施形態)

上述した実施形態では、図 3 に示す暗号化／認証付与装置 1 0 0 を一例に説明したが、暗号化及び認証情報の付与の順序はこれに限定されず、たとえば図 7 の暗号化／認証付与装置 6 0 0 に示すように、認証付与部 1 0 6 と暗号化部 1 0 4 の順序を逆にしてもよい。

【 0 0 7 4 】

また、上述した実施形態では、図 6 に示す復号／認証装置 2 0 0 を一例に説明

したが、認証確認および復号化の順序はこれに限定されず、たとえば図 7 の復号／認証装置 6 0 2 に示すように、暗号復号処理を認証処理に先立って行なうこととしても良い。

【 0 0 7 5 】

また、認証確認以降パケットそのものを処理せず、単に認証結果が正当であるかどうかだけを通知することとしても良い。たとえば、図 8 (a) に示すように復号／認証装置 2 0 0 が受信端末 8 0 2 に組み込まれている場合、送信端末 8 0 1 から伝送されたパケットは受信アプリケーション 8 0 3 にそのまま伝送され、認証装置 2 0 0 からは前記認証手段による認証の結果（たとえば受信されたビット系列が正当である場合、その旨）を通知する。この通知処理は、図 8 (b) に示すように復号／認証装置 2 0 0 が受信端末 8 0 2 と別体として構成されている場合には、復号／認証装置 2 0 0 から受信端末 8 0 2 に対して通知を行なうことにより実現できる。

【 0 0 7 6 】

以上述べた形態以外にも、種々の変形が可能である。しかしながら、その変形が特許請求の範囲に記載された技術思想に基づくものである限り、その変形は本発明の技術範囲内となる。

【 0 0 7 7 】

【発明の効果】

以上説明したように、本発明によれば、暗号鍵や認証鍵が破られることを防ぐことができ、通信システムにおけるデータ通信の安全性を向上することができる。

【 0 0 7 8 】

また、メディア情報の重要性の判断のような複雑な処理を行わず、パケット毎に選択的に暗号処理や認証処理を行なうため、従来の暗号処理や認証処理に必要であった計算量を低減することができる。結果として、オーバーヘッドを減少し、また処理遅延を回避できる。

【 0 0 7 9 】

さらに、暗号化におけるパディングや認証情報の付加による情報量の増大を抑

制することができる。

【図面の簡単な説明】

【図 1】

従来の暗号化の処理手順の一例を示す図である。

【図 2】

従来の認証情報付与の処理手順の一例を示す図である。

【図 3】

本発明の一実施形態に係る暗号化／認証付与装置の構成の一例を示すブロック図である。

【図 4】

本発明の一実施形態に係るビット系列の伝送の例を示す図である。

【図 5】

本発明の一実施形態に係るビット系列の伝送の例を示す図である。

【図 6】

本発明の一実施形態に係る復号／認証装置の構成の一例を示すブロック図である。

【図 7】

本発明の一実施形態に係る復号／認証装置の構成の一例を示すブロック図である。

【図 8】

本発明の一実施形態に係る、通知処理を行なう復号／認証装置の一例を示す図である。

【符号の説明】

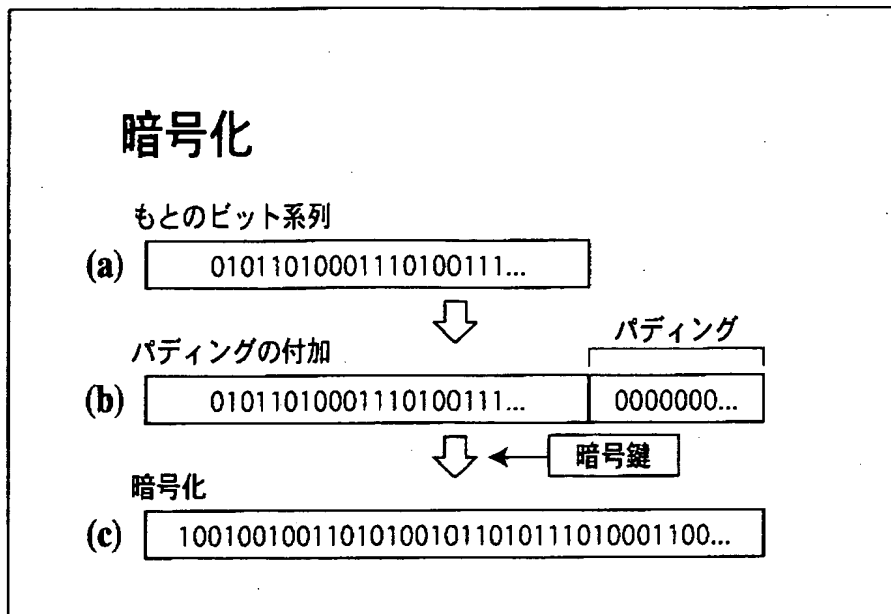
- 1 0 0 暗号化／認証付与装置
- 1 0 2 暗号・認証選択部
- 1 0 4 暗号化部
- 1 0 6 認証付与部
- 2 0 0 復号／認証装置
- 2 0 2 認証検出部

- 2 0 4 認証確認部
- 2 0 6 暗号検出部
- 2 0 8 暗号復号部
- 3 0 0 送信端末
- 3 0 2 有音部
- 3 0 4 無音部
- 4 0 0 受信端末
- 4 0 2 Pピクチャ
- 4 0 4 Bピクチャ
- 4 0 6 Iピクチャ
- 6 0 0 暗号化／認証付与装置
- 6 0 2 復号／認証装置
- 8 0 1 送信端末
- 8 0 2 受信端末
- 8 0 3 受信アプリケーション

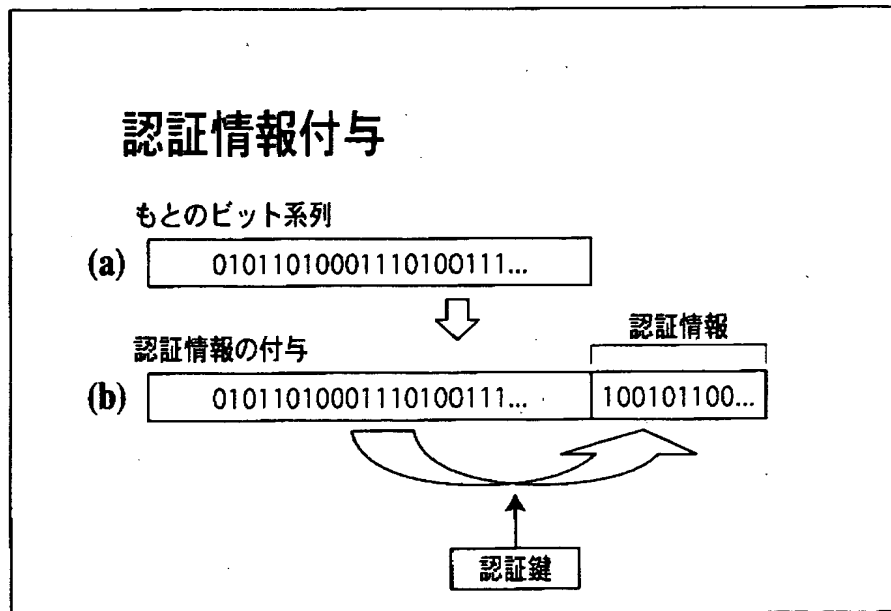
【書類名】

図面

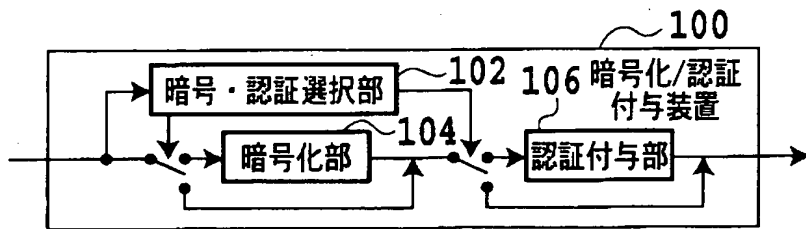
【図 1】



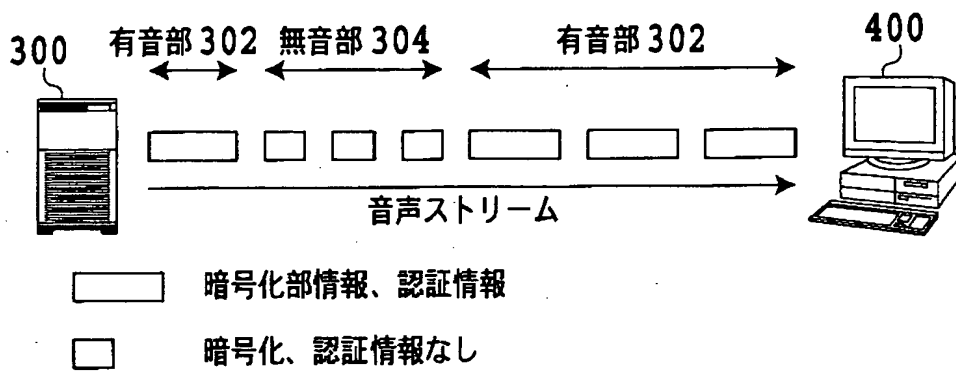
【図 2】



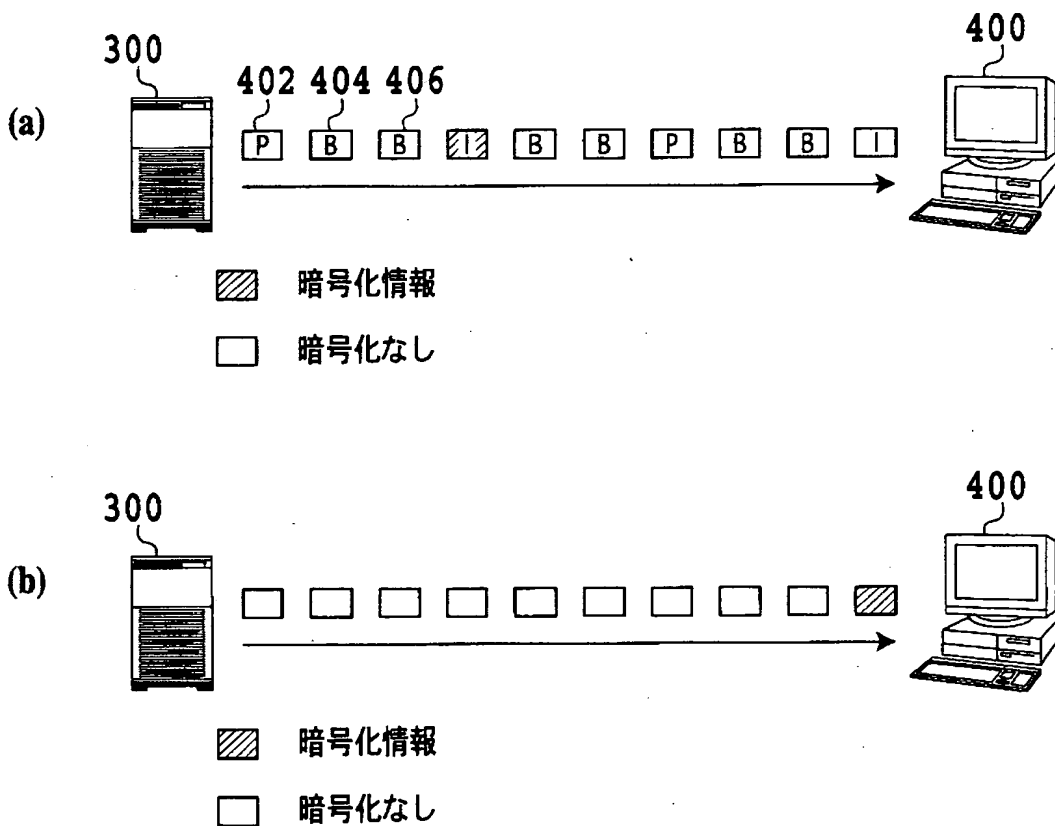
【図 3】



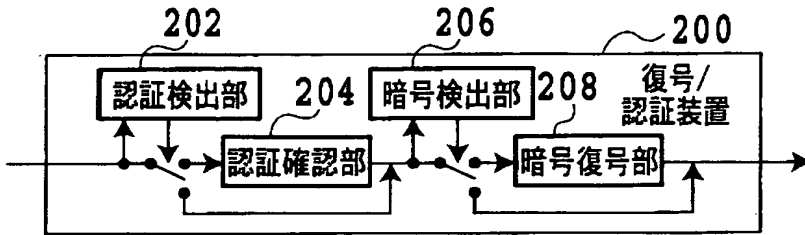
【図 4】



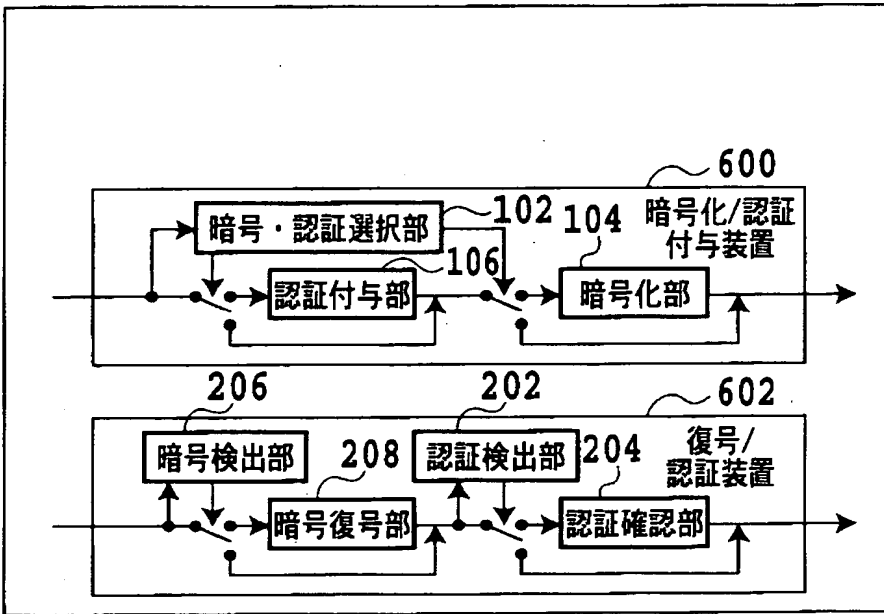
【図 5】



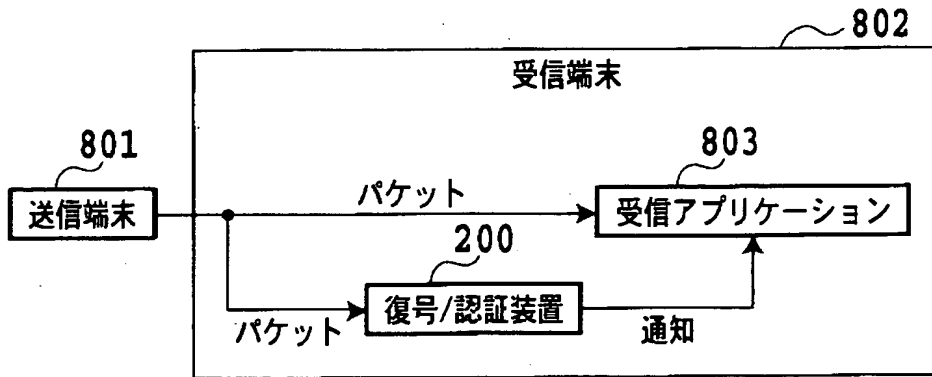
【図 6】



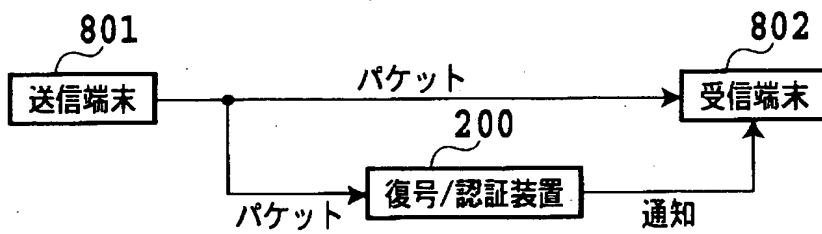
【図 7】



【図 8】



(a)



(b)

【書類名】 要約書

【要約】

【課題】 暗号鍵や認証鍵が破られるのを防ぐことができる暗号化装置および暗号化方法を提供する。

【解決手段】 送信端末 3 0 0 から受信端末 4 0 0 へ音声ストリームが送信されており、この音声ストリームのビット系列には、有音部 3 0 2 と、無音部 3 0 4 とが含まれている。有音部 3 0 2 には暗号化または認証情報の付与を行なう一方、無音部 3 0 4 には暗号化や認証情報の付加を行わず、そのまま伝送する。このように、ビット系列の種類に応じて選択的に暗号化または認証情報の付与を行なうことにより、暗号鍵や認証鍵が破られることを避けることができる。また、暗号処理や認証処理の処理量を減らし、情報量の増大を抑えることができる。

【選択図】 図 4

出 願 人 履 歴 情 報

識別番号 [392026693]

1. 変更年月日 2000年 5月19日

[変更理由] 名称変更

住 所 東京都千代田区永田町二丁目11番1号

氏 名 株式会社エヌ・ティ・ティ・ドコモ